IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF: Asus Atheros AR5B125 Laptop Computer, S/N: DCN0CV452335527	Case No. 5:20mj00012

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Justin P. Hasty, Special Agent of the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device described in Attachment A—which is currently in law enforcement possession in Winchester, Virginia, which is within the Western District of Virginia, and the extraction from that property of electronically stored information described in Attachment B.

2. I was hired by the FBI in February 2012 and successfully completed new agent training at the FBI Academy in Quantico, Virginia in July 2012. I am currently assigned to the Winchester Resident Agency of the Richmond Field Office. As a Special Agent of the FBI, I have investigated violations of federal law, including those related to child exploitation and child pornography. I have gained experience and knowledge through investigations and training and from discussions with law enforcement officers with experience and training in the investigation of violations of federal law related to child exploitation and child pornography. During the course of child exploitation and child pornography investigations, I have had the opportunity to

observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256), primarily in the form of computer media.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have set forth the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 (possession, receipt, and distribution of child pornography) and 2252A (activities relating to material constitution or containing child pornography) will be found on the following device: Asus Atheros AR5B125 Laptop Computer, S/N: DCN0CV452335527 (Subject Device).

5. I make this affidavit in support of an application for a search warrant for the Subject Device, which is further described in Attachment A, for the items described in Attachment B. I believe that probable cause exists to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A is located in and within the Subject Device. Thus, as outlined below, and based on my training and experience, I believe there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in the Subject Device.

6. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the

FBI.

RELEVANT STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors:

a. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing any visual depiction of a minor engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer. This section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mail.

b. 18 U.S.C. § 2252(a)(4)(B) prohibits knowingly possessing or accessing with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contains any visual depiction of minors engaged in sexually explicit conduct that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported by any means including by computer.

c. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by

computer.

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

8. The following definitions apply to this Affidavit and attachments hereto:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only

by the user who sent/received such a message, or by the Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and

delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

g. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

m. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

o. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

p. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes,

motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

r. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

s. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

t. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

u. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-

Text Transport Protocol ("HTTP").

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

9. On March 3, 2016, a federal search warrant was executed at the residence of CHARLES GRIFFITH MOLER ("SUBJECT"). At the time, SUBJECT resided with his parents in Winchester, Virginia (RESIDENCE 1). The probable cause for the search warrant was based on an investigation that concluded a user of an internet account at the residence was linked to an online community of individuals who regularly sent and received child pornography via a website, PlayPen, that operated on an anonymous online network. There was probable cause to believe that a user of the Internet account at RESIDENCE 1 knowingly accessed with the intent to view child pornography on PlayPen.

The Network[1]

10. PlayPen operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.[2] Using the Network prevents someone

[1] The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

[2] Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

11. Websites that are accessible only to users within the Network can be set up within the Network and PlayPen was one such website. Accordingly, PlayPen could not generally be accessed through the traditional Internet.[3] Only a user who had installed the appropriate software on the user's computer could access PlayPen. Even after connecting to the Network, however, a user had to know the exact web address of PlayPen in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of PlayPen, obtain the web address for PlayPen, and click on a link to navigate to PlayPen. Rather, a user had to have obtained the web address for PlayPen directly from another source, such as other users of PlayPen, or from online postings describing both the sort of content available on PlayPen and its location. Accessing PlayPen therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon PlayPen without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

12. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around

[3] Due to a misconfiguration, prior to February 20, 2015, PlayPen was occasionally accessible through the traditional Internet. In order to access PlayPen in that manner, however, a user would have had to know the exact IP address of the computer server that hosted PlayPen, which information was not publicly available. As of on or about February 20, 2015, PlayPen was no longer accessible through the traditional Internet.

the world, thereby masking the user's actual IP address which could otherwise be used to identify a user.

13. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

Arrest and Subsequent Investigation

14. During the execution of the search warrant at RESIDENCE 1, SUBJECT was interviewed, and he admitted to using his Compaq laptop computer to access and download child pornography via sites residing on the Network. SUBJECT's Compaq laptop computer was seized and subsequent forensic examination revealed image and video files that depicted child pornography.

15. On January 31, 2020, SUBJECT was arrested pursuant to an arrest warrant issued in the Western District of Virginia. The arrest warrant stemmed from an indictment charging SUBJECT with one count of accessing one of more visual depictions of a minor engaged in sexually explicit conduct with the intent to view, in violation of 18 U.S.C. § 2252(a)(4)(B).

16. Following his arrest, SUBJECT was transported to the FBI Winchester Resident Agency where he was advised of his *Miranda* rights. SUBJECT waived his *Miranda* rights and agreed to speak with FBI agents.

17. SUBJECT stated he had downloaded a browser onto the Subject Device in order to access the Network. SUBJECT acknowledged he has continued to download child pornography via the Network, view it, masturbate to it or attempt to, and then delete it. Each time, SUBJECT deleted the files and emptied the computer's recycle bin, but he stated, "obviously, that stuff stays in the deep part of the computer."

18. SUBJECT stated as recently as the night of January 30, 2020, the night prior to his arrest, he used the Subject Device to access "Website B"[4] and downloaded a video. According to SUBJECT, the video depicted an approximately 13 or 14 year old girl stripping and performing oral sex on an adult male who then had vaginal intercourse with the girl. In his estimation, the oldest the girl could have been was 16 years old. In addition, SUBJECT admitted to accessing child pornography websites via the traditional internet on the same night.

19. SUBJECT described another video from "Website B" that he viewed on the Device a few weeks prior to his arrest. According to SUBJECT, the video depicted an adult male having anal intercourse with a girl. SUBJECT estimated the girl's age to be 9, 10, or 11 years old.

[4] PlayPen was previously referred to as "Website A" in a related federal search warrant affidavit. On January 31, 2020, SUBJECT disclosed the name of a different website on the Network to FBI agents. For clarity, the website disclosed on January 31, 2020 will be referred to as "Website B." Disclosure of the name of the site would potentially alert its members to the fact that law enforcement is aware of its existence, potentially provoking members to notify other members of law enforcement's awareness, flee, and/or destroy evidence.

20. According to SUBJECT, "Website B" displayed separate categories that included children from ages 0 to 10 and teens from ages approximately 11 to 15, the latter of which was what SUBJECT usually selected. Within the 11 to 15 year old category, there were threads in which users posted videos for downloading, such as hardcore, solo, and scat. SUBJECT gave an example of hardcore as an adult male having "penetration sex, anally or vaginally" with a girl under the age of 18. SUBJECT gave additional examples of an adult male performing oral sex on an underage girl and an underage girl performing oral sex on a male who was usually an adult. SUBJECT preferred to view images or videos of girls who were 12, 13, or 14 years old.

21. SUBJECT indicated he had accessed "Website B" since late 2018, and he only accessed "Website B" with the Subject Device.

22. SUBJECT stated the Subject Device was located at his current residence in Winchester, Virginia (RESIDENCE 2), and he consented, in writing, to the search of RESIDENCE 2. In addition, SUBJECT was informed the purpose of the request was to seize the Subject Device.

23. The Subject Device is currently in the lawful possession of the FBI and in storage in Winchester, Virginia. In my training and experience, I know that the Subject Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Subject Device first came into the possession of the FBI.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

24. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I

have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view images of child pornography:

a. Individuals who access with intent to view child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Likewise, individuals who access with intent to view child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

c. Individuals who access with intent to view child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

d. Individuals who would have knowledge about how to access a hidden and embedded bulletin board could have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child

pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

e. Individuals who access with intent to view child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

25. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

26. Child pornographers can transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards can provide enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

27. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

28. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

29. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

30. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

31. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. There is probable cause to believe that things that were once stored on the Subject Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to access child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

35. *Nature of examination.* Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

36. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

37. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

38. Based upon the foregoing, I respectfully request that a search warrant be issued for the Subject Device, more particularly described in Attachment A, authorizing the search for items described in Attachment B.

Respectfully submitted,

/s/ Justin P. Hasty
Justin P. Hasty
Special Agent
Federal Bureau of Investigation

Received by reliable electronic means
and sworn and attested to by telephone on
February 19, 2020. 20, 2020:

HONORABLE JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Asus Atheros AR5B125 Laptop Computer, S/N: DCN0CV452335527, hereinafter the "Subject Device." The Subject Device is currently located in Winchester, Virginia in the possession of the FBI.

This warrant authorizes the forensic examination of the Subject Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The following items to be seized constitute contraband, fruits, instrumentalities, and evidence of crimes, to wit: violations of 18 U.S.C. §§ 2252 and 2252A relating to the receipt, distribution, possession of, and access with intent to view visual depictions of minors engaging in sexually explicit conduct and child pornography:

a. Child pornography;

b. Child erotica;

c. Visual depictions of minor engaged in sexually explicit conduct;

d. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to items "a" through "c" above (namely child pornography, child erotica, and visual depictions of minors engaged in sexually explicit conduct), or constituting evidence of or pertaining to the receipt, distribution, possession, transmission of, or access with intent to view through interstate or foreign commerce of items "a" and "c" above, or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children, including:

    i. Correspondence or communications, such as electronic mail, chat logs, and electronic messages;

    ii. Internet usage records, user names, logins, passwords, e-mail addresses and identities assumed for the purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records,

membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;

iii. Diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the computer and internet websites;

iv. Shared images, "friends lists" and "thumbnails;"

e. Evidence of who used, owned, or controlled the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

f. Evidence of software that would allow others to control the Subject Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. Evidence of the lack of such malicious software;

h. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

i. Evidence indicating the computer user's state of mind as it relates to the crime under investigation;

j. Evidence of the attachment to the Subject Device of other storage devices or similar containers for electronic evidence;

k. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Device;

l. Evidence of the times the Subject Device was used;

m. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Device;

n. Records of or information about Internet Protocol addresses used by the Device;

o. Records of or information about the Subject Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. Contextual information necessary to understand the evidence described in this attachment; and

q. Records, information, and items relating to the sexual exploitation of children on Website B and other such sites residing on the Network, including correspondence and communications between users of Website B or other such sites.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.